ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

A Survey of Black Hole Detection Techniques in WSNs

Sandeep Kumar[1], Dr.Suman Sangwan[2]

M.tech Student, Computer Science, DCRUST, Murthal, Sonepat, India [1]

Assistant Professor, Computer Science, DCRUST, Murthal, Sonepat, India [2]

Abstract: Wireless Sensor Networks (WSN) is a trending technology now-a-days and has a wide range of applications such as battlefield surveillance, traffic surveillance, forest fire detection, flood detection etc. But wireless sensor networks are susceptible to a variety of potential attacks which obstructs the normal operation of the network. Black hole attack is one of severe security threat that affects the network from its normal functioning by maliciously advertising itself having shortest route to the destination and then drops all receiving packets. There are lots of mechanisms have been proposed to defend network from black hole attack, but none of the solution looks most promising to defend against black hole attack. So in this paper, we have surveyed and compared the existing solutions to black hole attacks on AODV protocol. Tabular representation of comparison depicts clear picture of these solutions.

Keywords: AODV, Black hole attack, IDS, Routing

I. INTRODUCTION

A Wireless Sensor Network (WSN) consists of large number of sensor nodes working in cooperation manner to gather the information from the monitoring region. Generally WSN have little or no infrastructure. There are two types of WSNs: structured and unstructured [1]. In unstructured WSN there are huge numbers of nodes deployed randomly to monitor the region. Due to unavailability of physical presence on the region, network maintenance activities are difficult. In a structured WSN, all the nodes are deployed in fixed and planned manner. Positive point of a structured network is that fewer nodes can be deployed and requires fewer maintenance and management cost. In a WSN the object performing task of sensing is called a sensor. Sensor nodes are low power devices equipped with one or more sensors, processor, memory, power supply, a radio, and an actuator [2]. A variety of mechanical power, thermal sensor, biological, chemical,optical sensor, and magnetic sensors can be attached to enhance the power of sensor nodes [1]. Since the sensor nodes
have limited memory and are deployed in harsh environment and in difficult locations, radio transmitter is implemented to transfer the collected data to base station. WSNs have many applications such as military target tracking and surveillance, disaster relief, health monitoring, environment exploration seismic sensing to measure the environment.

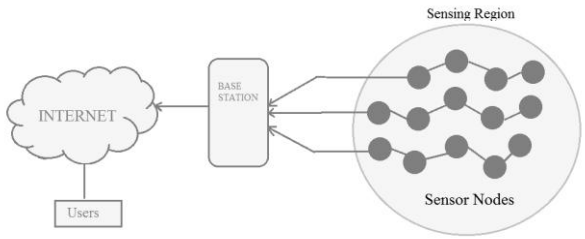

Figure 1.1 WSN model

The remainder of the paper is structured as follows. In next section we discuss about some constraints of WSN and fundamentals of security that are essential to be considered as key concepts before implementing any protocol. In Section 2, we discuss some of the possible attacks in WSN. Section 3 describes the Black hole attack in both reactive and proactive routing protocols. A review of existing techniques to handle black hole attack is presented in section 4. In section 5, Comparison of discussed techniques is performed. Finally, section 6 concludes the paper and points out future research directions.

II. CONSTRAINTS FOR WSNS

In the wireless sensor network, sensors are organized into the specific configuration to satisfy the requirements of ad-hoc applications. Unfortunately, the connectivity cannot remain unchanging at any working time. The sensor network is a broadcast network in which any signal can be captured by adversaries at any time. These features make wireless ad-hoc sensor networks more vulnerable than wired networks [2].
Resource Constraints:

Energy Constraints: Energy is one of the important constraints for WSNs. In sensor nodes energy consumption can be categorized in three parts: Sensor transducer, Communication among sensor nodes, microprocessor computation.

Memory Limitation: A sensor is a tiny device with a small amount of memory and storage space. Sensor nodes memory is usually includes flash memory and RAM (used for storing application programs, sensor info & intermediate results of computations). Usually, there is not sufficient space to run complicated programs or codes after loading the OS and application code.

Lack of Central Control: Because of resource constraints and network dynamics it is not feasible to have a central

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

point of control in sensor networks. Therefore security solutions must be decentralized and nodes must be able to achieve security [5].

Remote Locations: As sensor nodes are deployed in hard-to-reach locations so it will be infeasible to continuously monitor and protect the nodes from attacks. That why it will be difficult maintain a secure network.

Error-prone Communication: Unreliable communication is a dangerous threat to sensor security. Packets in WSNs may be lost due to collision, channel errors or routing failures. This may interfere with security mechanisms.

III. FUNDAMENTALS OF NETWORK SECURITY

Computer and network security is the collection of all policies, mechanisms, and services that protect a computer system or network from unauthorized access or unintended use. So, to ensure Network as secure some security mechanisms are applied that are Non-repudiation, Integrity, Availability, Privacy, Confidentiality, Authorization, Authentication, Freshness[3].

IV. ATTACKS IN WSN

There are different kinds of attacks possible by malicious nodes to harm the network and make the network unreliable for communication and proper functioning. Some of such kinds of attacks are:

a) *Jamming*: Jamming attack is related with disrupting or interfering the radio frequencies used by sensor nodes. Attacker may get physical access to some nodes and creates jam in the network to disrupt the network. Jamming attack come under physical layer attack.

b) *Tampering:* Refers to gaining physical access to a set of sensors by tampering with their hardware configuration and making nodes to act as adversary node. Tampering is possible at physical layer.

c) *Sybil Attack:* Sybil attack is defined as a malicious device illegitimately taking on multiple identities. In Sybil attack an adversary can appear to be in multiple places at the same time. A single node presents multiple identities to other nodes in the sensor network either by fabricating or stealing the identities of authenticated nodes. It is a Network layer attack.

d) *Wormhole attack:* Wormhole attack is a critical attack in which the attacker records the packets (or bits) at one location in the network and tunnels those to another location. This generates a false scenario that the original sender is in the neighbourhood of the remote location. The tunnelling procedure forms wormholes in a sensor network. The tunneling or retransmitting of bits could be done selectively.

e) *Hello Flood Attack:* Hello flood attack uses HELLO packets as a weapon to convince the sensors in WSN. In this type of attack an attacker with a high radio transmission range (termed as a laptop-class attacker) and processing power sends HELLO packets to a number of sensor nodes which are dispersed in a large area within a WSN.

f) *Black hole:* In Black hole attacks, a malicious node acts as a black hole to attract all the traffic in the sensor network through a compromised node or malicious node. A compromised node is placed at the center or any respective position, which looks attractive to neighboring nodes and attracts nearly all the traffic of surrounding nodes that was destined for a base station.

Black hole attack:

V. BLACK HOLE ATTACK

In this attack, a malicious node falsely advertises optimal paths (e.g. the shortest path or the most stable path) to the destination node during the path-finding process (in reactive routing protocols), or in the route updates messages (in proactive routing protocols). The intention of the malicious node could be to hinder the path-finding process or to intercept all data packets being sent to the destination node. A more delicate form of this attack is known as the grayhole attack, where the malicious node intermittently drops the data packets thereby making its detection even more difficult [4].

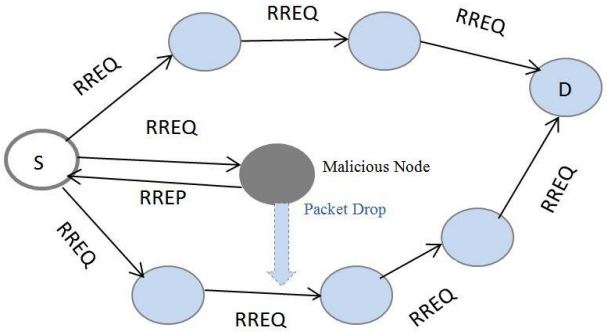

Figure 2. Black Hole Attack

Black hole attacks are classified into two categories:

- *Single Black Hole Attack*: In single black hole attack only one node act as malicious or compromised node which misbehaves within the network. It is also known as black hole attack with single malicious node.
- *Collaborative Black Hole Attack:* In collaborative black hole attack multiple nodes behaves as malicious node in the network and work in co-operative manner. It is also known as the black hole attack with multiple malicious nodes.

VI. SURVEY OF BLACK HOLE DETECTION TECHNIQUES

S. A. Arunmozhi et.al. [4] Discussed a defence scheme for detecting black hole node. The detection is based on the timing information and destination sequence numbers that is maintained in the Neighbourhood Route Monitoring Table. The table manages the record of time of Reply. A black hole node will send a route reply message without checking the routing table as the legitimate node normally does. This reduced reply time is used to detect the black hole node. To improve the security further, the destination sequence number is checked with the threshold value, which is dynamically updated. This protocol not only detects black hole attack but also improves the overall performance. Limitation is that it cannot prevent the

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

network from co-operative black hole attack because of assumption that black hole node cannot work in group.

SwarnaliHazra et.al. [5] proposed a trusted on-demand routing approach to prevent black hole attack depending on their trust model with different levels of trust computations. In this approach, black hole attackers are identified and isolated on context of data forwarding.

Fei Shi et.al [6] provides a cluster-based scheme form preventing black hole attacks in MANETs. It first employee's a powerful analytic hierarchy process (AHP) methodology to elect cluster heads (CHs). Then CHs are required to implement the black hole attack prevention scheme to not only detect the existence of black hole attacks but also identify the black hole nodes. Positive point with this scheme is that it is feasible and efficient in preventing black hole attacks.

R. TANUJA et al. [7] this article propose technique to eliminate Black Hole and False Data Injection attacks initiated by the compromised inside nodes and outside malicious nodes respectively using a new acknowledge scheme with low overhead. Advantage with this scheme is that it can successfully identify and eliminate 100 % black hole nodes and ensures more than 99 % packet delivery with increased network traffic.

Harsh Pratap Singh and Rashmi Singh [8] has proposed broadcast synchronization (BS) and relative distance (RD) method of clock synchronization which is used to prevent the black hole nodes. BS (Broadcast Synchronization) is very famous technique for clock synchronization process in Mobile-ad hoc Network. This paper has BS technique for removal of cooperative black hole attack. Sometimes the detection process for worms is failed in the clock synchronization. In this case this paper imposed another method for black hole detection using Relative Velocity distance.

Ming-Yang Su[9] in this several IDS (intrusion detection system) nodes are deployed in MANETs in order to detect and prevent selective black hole attacks. The IDS nodes must be set in sniff mode in order to perform the so-called ABM (Anti-Black hole Mechanism) function, which is mainly used to estimate a suspicious value of a node according to the abnormal difference between the routing messages transmitted from the node. When a suspicious value exceeds a threshold, an IDS nearby will broadcast a block message, informing all nodes on the network, asking them to cooperatively isolate the malicious node. This study employs ns2 to validate the effect of the proposed IDS deployment, as IDS nodes can rapidly block a malicious node, without false positives, if a proper threshold is set. Advantage with this is that it is multipath passed protocol and packet loss rate can be decreased to 11.28% and 14.76%. Drawbacks: Failed at co-operative black hole attack detection.

Muhammad Raza et.al [10] They have proposed a novel architecture of FRIMM (A Forced Routing Information Modification Model) prevents black hole attacks in wireless Ad Hoc network by introducing automatic error correction in routing information that leads the node to select correct path thus secure transmission will take place between source and destination.

*NeelamKhemariya et.al [11]*have proposed an algorithm and it is implemented on AODV (Ad hoc on demand Distance Vector) Routing protocol. The algorithm can detects both the single Black hole attack and the Cooperative Black hole attack. These algorithms first identify black hole nodes from the network and then remove their entries from the routing table. The advantage of the algorithm is that it not only detects the black hole nodes in case when the node is not idle but it can also detect the Black hole nodes in case when a node is idle as well.

SubhashisBanerjee,MousumiSardar et.al[12] have proposed trust based mechanism for detection and mitigation of black hole nodes from the network. They have introduced mechanism which detects malicious nodes from the network without introducing additional control packets and without modifying routing table. Detection is originator initiated hence there is no need to rely on intermediate nodes. Trust mechanism

KashifSaghar et.al[13] have proposed RAEED (Robust formally Analyzed protocol for wireless sensor networks Deployment), which is able to address the problem of black hole attacks using formal modeling and proves that RAEED avoids such kind of attacks.

SatyajayantMisra et.al[14] have propose an efficient technique that uses multiple base stations deployed in the network to counter the impact of black holes on data transmission their work is based on how to deploy the base stations for collecting the information gathered by nodes deployed in hostile environment. Simulation shows packet delivery ratio was 99% and detection rate was 100% but no. of base stations was not optimal.

Sonika Malik et.al [15] Have proposed the solution to black hole attack by using data routing table that stores routing information of neighbor nodes. This analyze the data routing table of nodes and send check packet to the neighbor nodes to get the information about nodes and from this information they finds the trust worthy and reliable nodes and eliminate the malicious black hole nodes by rising global alarm to warn the network about malicious nodes.

Anurag Gupta et.al[16] Have proposed the solution to avoid denial of service and black hole attack in mobile adhoc network. In this the solution to detect the malicious node has been presented, for that all nodes in the network are listed together and counter clock is applied to every node and any misbehavior is detected by using RREQ time, Current time, Expire time Source sequence number and Destination Sequence number. Malicious nodes are added to malicious list and when session expires malicious nodes are removed from malicious list because they assume that after some time malicious node stops doing malicious activity.

Anishi Gupta [17] Proposed a new method MEAODV(Modified Enhanced AODV), based on EAODV(Enhanced AODV).The MEAODV is based on route discovery process for mitigating black hole effect. It does not have any overhead to the network. The similar logic is used as in EAODV but has few different condition parameters for checking the RREP message for better

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

route discovery mechanism. Performance is compared with EAODV and performance delivery ratio is slightly higher. But negative point is that it does not consider co-operative Black hole attack.

H.Shafieiet.al[18] proposed two techniques to detect sinkholes in the network. In the first approach, base station samples the residual energy of sensing nodes deployment region using a geostatistical method and estimates a parameter called statistical estimator. Base station utilizes this parameter to estimate the presence of energy holes in deployment region using geostatistical frailty survival model. Energy holes around the base station are neglected whereas presence of energy holes in rest of the network ensures occurrence (presence/ existence) of sinkholes in network. Base station then instructs all of network nodes to avoid the suspicious region in their routing to mitigate the attack or ignore it. Second approach is Distributed monitoring method comprising two phases: Distributed residual energy query phase and Distributed estimation and detection phase. Distributed monitoring method detects region with lower average residual energy level and applies a mitigation method to eliminate sinkholes.

S. S. Bajwa and M. K. Khan [19] proposed Grouped Black Hole Attack Security Model (GBHASM) to prevent grouped black hole attacks in Ad hoc On-demand Distance vector (AODV) protocol in wireless ad hoc networks. This model is based on two modules. First module describes how a new node becomes member of network. After having joined the network, this node is assigned node code (NC) pkk1 and pkk2. When node requests for shortest path to destination with a packet having pkk2, then each node matches Node Code pkk1 with pkk2. If they match within Time to Live (TTL), routing information is shared with intermediate node otherwise packet is forwarded to next node. This model has low delay and high performance.

Varshney et al., [20] proposed a monitoring method called Watchdog AODV mechanism to form detect black hole nodes in mobile adhocnetworks.In this method nodes act as watchdogs monitor their neighbors locally using control messages by listening to all nodes within transmission range to detect misbehaving as well as black hole node. Black hole node once detected, is excluded from the path of transmitting messages. Limitation of Watchdog AODV is that it is vulnerable to attack of two consecutive nodes. It can monitor only first node while the consecutive node performs attack. Watchdog AODV has higher packet delivery ratio and lower overhead than AODV.

M. Mohanpriya, I. Krishanamurthi [21] presented Modified Dynamic Source Routing protocol (MDSR) to detect and prevent selective black hole attack by analyzing forwarding behavior of nodes. This approach detects the presence of gray hole attackers in source route based on difference between number of packets source node sends and number of packets that are actually received by destination. IDS nodes deployed in network broadcast the block message to all nodes and then suspected malicious nodes are isolated from the routing path as well as network. Advantages of MDSR are that it reduces packet drop ratio by 64 % but increased overhead ratio by 8 %.MDSR has less end to end delay as compared to DSR protocol.

S. Vidhyaand T. Sasilatha [23] proposed a black hole detection scheme in wireless sensor network by adding energy to sensor nodes externally through batteries that increases network lifetime. The author provided a solution to black hole attack by a public key encryption through Message Digest MD5 cryptographic function with 128 bithash value. While relaying messages from source to destination, confidentiality, authenticity and integrity of data packets is to be kept in mind. Nodes are in network in such a way that a node acting as a mobile agent monitors the activities of neighboring nodes and informs trust manager about any changes in status of nodes. Trust manager verifies identity of each node in the network and intimates to neighbors about the malicious behavior of a node if it finds any to keep the network safe. MD5 marks a node malicious if it uses another node's signature and packets are forwarded to neighbors through alternate route. Providing energy externally increases network lifetime, packet delivery ratio, as well as throughput.

N. Chaudhary and L. Tharani [24] proposed a Timer based detection mechanism to detect and eliminate black hole nodes launched over AODV in mobile adhoc networks. This scheme utilizes a trust value defined by every node on its neighbors. Initially all neighbors are assigned max_trust value and a timer is set with each data packet. A node does not communicate with its neighbor if neighbor's trust value is less than min trust. The node checks by listening to wireless transmission whether have been received by next hop before timer expires. If node could not hear wireless transmission of next hop, it reduces trust value of next hop and broadcasts this information to all nodes in network so that they can update their routing tables. If node's next hop continues to drop packets, its trust value goes on decreasing and becomes less than min_trust. All nodes in network put such a node in their blacklist table. In this way, all blackhole nodes get eliminated from the network. Packet delivery ratio gets improved as black hole nodes are detected and removed from the network.

Siddiqua et al., [25] proposed a secure knowledge algorithm to detect and mitigate black hole attack on AODV by taking packet drop reasons into consideration before declaring a trusted node as black hole node. Each node monitors the behavior of its neighbor by listening to packet transmission wirelessly. Every node compares the neighbor information with its knowledge table information. The nodes monitor the control packets as well as data packets to prevent selective dropping. When packet dropping reaches to a threshold then before declaring a node to be malicious the algorithm first checks whether suspected node is destination or not. It also checks packet drop reasons such as Time to live (TTL) and residual energy. If suspected node is detected to be a black hole, its id is broadcasted to all other nodes in network so that malicious node can be avoided in routing process. Secure AODV shows better performance in terms of throughput and delay as compared to existing AODV.

DOI 10.17148/IJARCCE.2015.45119

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

VII. COMPARISON

Various techniques are discussed based on various criteria, which are base routing protocol used, Modifies routing table or not, new control packets introduced or not, type of black hole detected and simulation tool used.

Sr No.	Technique	Routing Protocol Used	Modifies Routing Table (YES/NO)	New Control Packets (YES/NO)	Simulation TOOL	Performance Matrices	Results	Year
1.	NRMT[4]	AODV	YES	YES	NS2	Routing overhead, PDR, CPU usage, Memory usage, Delay	Network Performance Improved	2012
2.	CST-AODV [5]	AODV	YES	YES	-	Packet loss Rate	Packet Loss Rate are negligible	2014
3.	Cluster Based [6]	AODV	YES	NO	NS2	PDR v/s traffic load	Improved Packet delivery ratio under black hole attack.	2013
4.	BHnFDIA [7]	MAC	NO	YES	MATLAB	PDR v/s compromised nodes	Gives 100% packet filtering efficiency and 99% packet delivery ratio	2013
5.	Secure Path Based[8]	OLSR	YES	YES	NS2	Throughput end to end delay, PDR, Jitter	Effective performance in terms of PDR, Throughput, end to end delay	2014
6.	IDS Based[9]	AODV	YES	YES	NS2	Total packet loss rate	Packet loss reduced to 10.05% and detection rate 100%	2011
7.	FRIMM[10]	AODV	YES	NO	-	-	-	2011
8.	Neelam et.al [11]	AODV	NO	YES	NS2	Throughput, PDR, end to end delay	Improve network performance	2013
9.	Trust Based[12]	AODV	NO	NO	-	-	-	2013
10.	RAEED [13]	INSENS	YES	NO	TOSSIM	% of nodes blocked	Robust and lower overhead	2014
11.	BAMBi[14]	-	NO	NO	Realistic simulation	Packet delivery success, packet delivery failure	Packet delivery ratio is 99% Detection ratio is 100%	2011
12.	Alarm Based[15]	AODV	YES	YES	NS2	-	-	
13.	DSN Based[16]	AODV	YES	YES	NS2	Throughput, end to end delay	Better throughput and end to end delay	2015
14.	MEAODV[17]	AODV	YES	YES	NS2	PDR, end to end delay, no. of malicious nodes.	Better PDR as compared to EAODV	2013
15.	Geostatistical based[18]	AODV	NO	NO	OMNET++	False positive false negative	Adopted 95% confidence level	2014
16.	GBHASM[19]	AODV	YES	YES	NS2	No. of RREQ and RREP	High performance less delay	2010
17.	Watchdog AODV[20]	AODV	YES	YES	NS2	PDR, MAC load, end to end delay	Improved PDR and end to end delay	2014
18.	MDSR[21]	DSR	YES	YES	GLOMOSIM	Packet drop ratio, end to end delay, PDR, overhead	Percentage of Packet loss rate is better	2013
19.	ACK based[22]	AODV	NO	YES	OPNET			2014
20.	MD5 based[23]	AODV	NO	NO	NS2	PDR, Throughput, end to end delay	Improved overall network performance	2014
21.	Timer based[24]	AODV	YES	YES	EXata-cyber	PDR v/s no. of attacker	Improved PDR	2015
22.	Knowledge based[25]	AODV	YES	YES	NS2	PDR v/s no. of malicious nodes	Effective PDR	2015

VIII. CONCLUSION

Wireless Sensor Networks are vulnerable to many types of attacks due to deployment of sensor nodes in an unattended environment. These types of networks are suffered from the black hole attack as there is no centralized security management. This paper provided a survey on various countermeasures for black hole attack. In this survey, firstly we have given the security goals of a network. Next, we have presented some of the possible network layer attacks in WSNs. This survey also gives the tabular analysis of various security mechanisms to prevent network from black hole attack. It is to be believed that this survey will help future researches in developing a good knowledge about the attacks and their countermeasures.

REFERENCES

[1] Di Pietro, R., S. Guarino, N. V. Verde, and J. Domingo-Ferrer, "Security in wireless ad-hoc networks–A survey," Computer Communications, Vol. 51, pp. 1-20, 2014.

[2] Kifayat, Kashif, MadjidMerabti, Qi Shi, and David Llewellyn-Jones. "Security in wireless sensor networks." In Handbook of Information and Communication Security, pp. 513-552. Springer Berlin Heidelberg, 2010.

[3] Shio Kumar Singh, M P Singh, D K Singh, "A Survey on Network Security and Attack Defense Mechanism For Wireless Sensor Networks", International Journal of Computer Trends and Technology- May to June Issue 2011.

[4] Arunmozhi, S. A., and Y. Venkataramani. "Black Hole Attack Detection and Performance Improvement in Mobile Ad-Hoc Network." Information Security Journal: A Global Perspective 21, no. 3 (2012): 150-158.

[5]] Hazra, Swarnali, and S. K. Setua. "Blackhole Attack Defending Trusted On-Demand Routing in Ad-Hoc Network." In Advanced Computing, Networking and Informatics-Volume 2, pp. 59-66. Springer International Publishing, 2014.

[6] Shi, Fei, Weijie Liu, Dongxu Jin, and Jooseok Song. "A cluster-based countermeasure against blackhole attacks in MANETs." Telecommunication Systems 57, no. 2 (2014): 119-136.

[7] Tanuja, R., M. K. Rekha, S. H. Manjula, K. R. Venugopal, S. S. Iyengar, and L. M. Patnaik. "Elimination of black hole and false data injection attacks in wireless sensor networks." In Proceedings of the Third International Conference on Trends in Information, Telecommunication and Computing, pp. 475-482. Springer New York, 2013.

[8] Singh, Harsh Pratap, and Rashmi Singh. "A mechanism for discovery and prevention of coopeartive black hole attack in mobile ad hoc network using AODV protocol." In Electronics and Communication Systems (ICECS), 2014 International Conference on, pp. 1-8. IEEE, 2014.

[9] Su, Ming-Yang. "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems." Computer Communications 34, no. 1 (2011): 107-117.

[10] Raza, Muhammad, and Syed IrfanHyder. "A forced routing information modification model for preventing black hole attacks in wireless Ad Hoc network." In Applied Sciences and Technology (IBCAST), 2012 9th International Bhurban Conference on, pp. 418-422. IEEE, 2012.

[11] Khemariya, Neelam, and Ajay Khuntetha. "An Efficient Algorithm for Detection of Blackhole Attack in AODV based MANETs." International Journal of Computer Applications 66, no. 18 (2013).

[12] Banerjee, Subhashis, MousumiSardar, and KoushikMajumder. "AODV Based Black-Hole Attack Mitigation in MANET." In Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2013, pp. 345-352. Springer International Publishing, 2014.

[13] Saghar, Kashif, David Kendall, and Ahmed Bouridane. "Application of formal modeling to detect black hole attacks in wireless sensor network routing protocols." In Applied Sciences and Technology (IBCAST), 2014 11th International Bhurban Conference on, pp. 191-194. IEEE, 2014.

[14] Misra, Satyajayant, KabiBhattarai, and GuoliangXue. "BAMBi: blackhole attacks mitigation with multiple base stations in wireless sensor networks." InCommunications (ICC), 2011 IEEE International Conference on, pp. 1-5. IEEE, 2011.

[15] Malik, Sonika, and InduKashyap. "Identifying, Avoidance and Performance Assessment of Black Hole Attack on AODV Protocol in MANET." International Journal of Computer Applications 95, no. 17 (2014): 6-11.

[16] Gupta, Anurag, Bhupendra Patel, Kamlesh Rana, and Rahul Pradhan. "Improved AODV Performance in DOS and Black Hole Attack Environment." In Computational Intelligence in Data Mining-Volume 2, pp. 541-549. Springer India, 2015.

[17] Gupta, Anishi. "Department of Computer of Engineering, Delhi Technological University, New Delhi, India." In Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference on, pp. 1-6. IEEE, 2013.

[18] Taylor, Vincent F., and Daniel T. Fokum. "Mitigating black hole attacks in wireless sensor networks using node-resident expert

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

systems." In Wireless Telecommunications Symposium (WTS), 2014, pp. 1-7. IEEE, 2014.

[19] Bajwa, ShahidShehzad, and Muhammad Khalid Khan. "Grouped Black hole Attacks Security Model (GBHASM) for Wireless Ad-Hoc Networks." In Computer and Automation Engineering (ICCAE), 2010 The 2nd International Conference on, vol. 1, pp. 756-760. IEEE, 2010.

[20] Varshney, Tarun, Tushar Sharma, and Pankaj Sharma. "Implementation of Watchdog Protocol with AODV in Mobile Ad Hoc Network." In Communication Systems and Network Technologies (CSNT), 2014 Fourth International Conference on, pp. 217-221. IEEE, 2014.

[21] Mohanapriya, M., and IlangoKrishnamurthi. "Modified DSR protocol for detection and removal of selective black hole attack in MANET." Computers & Electrical Engineering 40, no. 2 (2014): 530-538.

[22] Baadache, Abderrahmane, and Ali Belmehdi. "Struggling against simple and cooperative black hole attacks in multi-hop wireless ad hoc networks." Computer Networks 73 (2014): 173-184.

[23] S. Vidhyaand T. Sasilatha, "Performance Analysis of Black Hole Attack DetectionScheme using MD5 Algorithm in WSN " , IEEE International Conference on Smart Structures & Systems (ICSSS-2014), Chennai-INDIA. pp. 51-54

[24] N. Chaudhary and L. Tharani , " Preventing Black Hole Attack in AODV using Timer-Based Detection Mechanism", SPACES-2015, Dept of ECE, K L UNIVERSITY, 2015, pp. 1-4

[25] Siddiqua et al., "Preventing Black Hole Attacks in MANETs Using Secure Knowledge Algorithm", SPACES-2015, Dept of ECE, K L UNIVERSITY, 2015, pp. 421-425.